



*Virginia Information Technologies Agency*



# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

October 23, 2008





# OCTOBER





# ISOAG October 2008 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, VITA
II.	Security Awareness	Peggy Ward, VITA
III.	Center for Internet Security	Bert Miuccio, CIS President/CEO
IV.	Playing Safely in the Cloud	Marie Greenberg, SCC
V.	Safely Playing in the Cloud	Steve Werby, VCU
VI.	Commonwealth Security Information Resource Center	Michael Watson, VITA
VII.	Cleaning Up SQL Injections	Michael Watson, VITA
VIII.	ITP Security UPDATE	Bill Ross, Northrop Grumman
VI.	New Guidelines	Cathie Brown, VITA
VII.	Commonwealth Security Annual Report	Peggy Ward, VITA





*Virginia Information Technologies Agency*

# Information Security Awareness

**Peggy Ward**

**Chief Information Security &  
Internal Audit Officer**





# Information Security Awareness Month

**Governor Kaine** has signed a proclamation designating

**October, 2008**

as

**Information Security Awareness Month**

in the

**Commonwealth of Virginia!!**



## 2008 Information Security Awareness Tools

The Information Security Toolkit has been updated with new materials

For printing cost estimates you can contact DMV's Damian McInerney @  
367-0925

***Thank you DMV!***





# Information Security Awareness

- **Video**

- “The Duhs of Security”
- Video length: 12 minutes

- **Availability**

- Early November: Knowledge Center and YouTube
- Late November: DVD

# The Center for Internet Security

*“Measurably reducing risk through collaboration,  
consensus, & practical security management”*



**Bert Miuccio, President/CEO**





# Content of this Presentation:

- I. CIS Background
- II. CIS Consensus Benchmarks
  - their value to system and network security
- III. CIS Audit Tools (primarily CIS-CAT)
  - use cases & features
  - specs & system requirements
- IV. Consensus Information Security Metrics
  - CIS Information Security Metrics Service
- V. The Rights & Benefits of CIS Membership

# CIS Background



# The Center for Internet Security (CIS)

- Formed in October 2000
- A not-for-profit consortium of users, security consultants, and vendors of security software (CIS Members)
- Convenes and facilitates teams developing consensus Benchmarks for system & network security configuration
- Developed and distributes the CIS Configuration Assessment Tool (CIS-CAT) to its members
- Convenes and facilitates teams developing consensus information security metrics



# CIS Consensus Benchmarks





## The Consensus Benchmarks Are:

- **Recommended technical control rules/values for hardening OSs, applications, and network devices.**
- **Downloaded over 1,000,000 times per year.**
- **Distributed in .pdf to the general public (to propagate their use/adoption worldwide)**
- **Distributed in XML (XCCDF) format to CIS Members.**
- **Used by thousands of organizations worldwide as the basis for their security configuration policies and the standard against which to compare them.**

# The Security Value of Consensus Benchmarks

## The Problem:

The vast majority of cyber attacks exploit known software flaws for which a patch or security configuration control is known.

## The Solution:

Research and Case studies show that 80-95% of known vulnerabilities are blocked by the technical security controls and actions recommended in the consensus benchmarks.

**(research reports & case studies are on the CIS web site)**

# The Compliance Value of Consensus Benchmarks

## The Problem:

Regulatory requirements for information security are burgeoning. Some explicitly require adoption of configuration best practices (FISMA, PCI), others do so implicitly (ISO, SOx, etc.)

## The Solution:

The benchmarks distributed by CIS are the ONLY consensus best practice standards for security configuration both developed and accepted by business/industry and government internationally.

## The CIS Consensus Process:

- Form teams of security subject matter experts
- Develop initial benchmark draft
- Build consensus via draft review & discussion (mail list & teleconference communication)
- Develop an Audit Tool for selected benchmarks
- Update each Benchmark periodically based on extensive user feedback



# Vendors are Fully Engaged in the Consensus Process

- Microsoft
- Sun
- HP
- Cisco
- Oracle
- Apple
- IBM
- Juniper
- Novell
- Checkpoint
- Red Hat
- CIS does not accept funding from software vendors

# **40 Benchmarks are Now Available In .pdf Format ONLY at the CIS Public Web Site:**

**[www.CISecurity.org](http://www.CISecurity.org)**

- Twenty are for operating systems
- Sixteen are for middleware and applications
- Four are for network devices

# CIS Operating System Benchmarks

- WinXP Pro (SP1/SP2)
- Windows Server 2003
- Windows 2000 Pro
- Windows 2000 Server
- Windows 2000
- Windows NT
- Mac OS X 10.5 (Leopard)
- Mac OS X 10.4 (Tiger)
- FreeBSD
- Solaris 10
- Solaris 10 11/06 and 8/07
- Solaris 2.5.1 – 9.0
- HP-UX
- AIX
- Red Hat Linux 5 (RHEL 5)
- Red Hat Linux 4 (for RHEL 2.1, 3.0, 4.0 and Fedora Core 1,2,3,4, & 5)
- SUSE Linux
- Slackware Linux
- Debian Linux
- Novel OES: Netware

# CIS Application Benchmarks

- Exchange Server 2003
- Exchange Server 2007
- Oracle Database 8i
- Oracle Database 9i/10g
- Oracle Database 11g
- Apache Web Server
- MySQL
- SQL Server 2005
- SQL Server 2000
- BIND
- Novel eDirectory
- IIS
- OpenLDAP
- FreeRADIUS
- Virtual Machine
- Xen Server
- VMWare ESX Server



# CIS Network Device Benchmarks

- Wireless Networks
- Cisco IOS Router
- Cisco ASA, FWSM, and PIX
- Check Point Firewall

# Benchmarks Now in Development

## New:

- Apache Tomcat
- Print Devices
- Microsoft Office 2003/2007
- Microsoft Office SharePoint Server 2007 (MOSS)
- Juniper JunOS
- SharePoint 2007
- Sybase
- VoIP
- Web Browsers

## Updates:

- Redhat Enterprise Linux 5
- SQL 2005
- VMware ESX Server
- Windows 2003 DC/MS

**14 of the 40 Benchmarks are Available  
To Members Only  
In Machine-Readable XML (XCCDF) Format  
For Use With CIS-CAT  
And Tools that Members Develop**

**The XML Benchmarks are Available  
On the CIS Members Web Site at:**

**<http://members.cisecurity.org>**

# How **YOU** Can Be Involved In the Benchmark Consensus Process

- Participate in the Benchmark consensus process
- Lead teams developing or updating benchmarks
- Continuously tell CIS what new Benchmarks and other security resources you need
- Be active in the CIS member forums
- Provide feedback regarding CIS-CAT (feature requests & bugs)



# CIS Audit Tools



# CIS Audit Tools Use Cases

- Improve security awareness by comparing security of “out-of-the-box” vs. hardened systems.
- Create standard configuration images for hardening systems prior to deployment
- Periodically audit and/or routinely monitor the configuration of individual production systems compared to the Benchmark and/or enterprise policies.
- Audit/monitor multiple systems simultaneously using system management utilities (Members must devise/script their own method – CIS does not provide one)

# CIS-CAT

## (CIS-Configuration Audit Tool)

- Host based, configuration assessment/audit software tool
- Available ONLY to CIS Members – distributed via the CIS Members web site
- Distributed with GUI & CLI
- The ONLY tool CIS is currently developing & supporting
- Requires JRE v1.5
- CIS-CAT and JRE v1.5 can reside on target system, removable drive, or network drive, provided it is accessible from the target of evaluation.



# CIS-CAT

- A Java tool that reads the Benchmark XML files (XML files specify the Benchmark rules and values, and the checks that the tool executes to assess & report configuration status)
- Also reads customized XML files - compare the configuration of systems with both the CIS Benchmarks and customized configuration policies
- Is undergoing NIST Validation Testing for FDCC and other SCAP configuration policy content



# CIS-CAT Now Supports These Benchmarks:

- Windows XP
- Windows Server 2003
- Vista (NIST SCAP Content)
- SuSE
- Slackware
- Red Hat Enterprise Linux 5 (RHEL 5)
- Red Hat Enterprise Linux 4 (2.1, 3.0, 4.0 & Fedora Core 1-5)
- Debian
- AIX
- HP-UX
- FreeBSD
- Solaris 10 11/06 and 8/07 (Benchmark v1.0)
- Solaris 2.5.1 – 9.0
- Oracle 9i/10g on Windows and UNIX

# CIS-CAT Documentation

- README file in the download package
- Specification document distributed via the members site.
- CIS-CAT Users Manual distributed via the members site.
- A guide to assist users in modifying the Benchmark XML files for use with CIS-CAT
- Additional guidance is provided via the member discussion forum

# Other CIS Audit Tools Currently Available

- Router Audit Tool (RAT Tool)
- Perl tools for Unix operating systems
- Apache benchmark tool
- Oracle Database 8i tool
- CIS no longer maintains or provides user support for any of these tools
- They will reach end of life when the Benchmarks for which they were created become out of date and are no longer distributed

# Consensus Metrics for Information Security and the CIS Security Metrics Service





# What is a Metric?

- A standard of measurement that facilitates the quantification of some particular characteristic.
- Enables repeatable measurement
- Some examples in business:
  - Profit Margin - (finance & accounting)
  - Transit time - (transportation & logistics)
  - Cost per click – (advertising & marketing)
  - Customer Satisfaction – (business & marketing)
  - Post Surgical Infection Rate – (Healthcare & Insurance)

# CIS Security Metrics Initiative

- Organizations struggle to make cost-effective security investment decisions;
- Information Security Professionals **lack widely accepted and unambiguous metrics** for decision support.
- CIS has established a **consensus team of industry experts** to address this need.
- The result will be an **independent, metric framework and service** to define, collect and analyze data on security process benefits and outcomes.

## Goals for 2008

- Reach consensus on a small, initial set (<10) of unambiguous and widely accepted security metrics
  - **Facilitate widespread adoption among CIS Members**
- Launch a security metrics service that enables:
  - **Communication of enterprise security status over time**
  - **Anonymous, inter-enterprise comparison of security status**
  - **Widely understood and proven correlation of effective security practices and security performance**

# Consensus-Based Metrics for Information Security

- **User-originated, unambiguous methods** for measuring key aspects of the information security status of an enterprise.
- **Defined through collaboration** among a large group of security experts from leading commercial, government and academic organizations.
- **Help enterprises** correlate implementation of security practices with outcomes and make better informed security investment decisions.



# Initial Consensus Metrics

Key criteria were established for the initial set. They are a balanced combination of outcome and practice metrics measuring:

- Outcome
  - Mean-Time To Discovery of security incidents
  - Mean-Time To Recovery from security incidents
  - % of Incidents detected by internal controls
- Process / Practice / Diagnostic Metrics
  - % of systems configured to approved standards
  - % of systems patched to policy
  - % of systems with anti-virus software enabled
  - % of business applications that had a risk assessment
  - % of business applications that had a penetration or vulnerability assessment
  - % of application code that had a security assessment, threat model analysis, or code review prior to deployment

# CIS Information Security Metrics Service

- A software-based service that will provide value to enterprises by enabling:
  - Mechanisms for correlating security practices with outcomes
  - Communication of security performance over time
  - Anonymous intra and cross-organization comparison of security status

# CIS Information Security Metrics Service – Some Requirements for Market Success

- Privacy and assurance that individual data values cannot be traced back to the submitters identity;
- Protect against the submission of non-legitimate data by non-legitimate submitters;
- Provide a robust set of analysis and reporting features.

# Milestones

- ✓ Reach consensus on an initial set of security metrics
- ✓ Reach consensus on final definitions and conform them to the consensus schema – Q3 & Q4
- ❑ Launch CIS Security Metrics & Benchmarking Service – Q4
- ❑ CIS Members contributing data and producing reports – Q4



# Questions?

- What are your organizations top three (3) information security metrics?
- How are you tracking incidents? To what detail?
- How important are security metrics for The Commonwealth of Virginia & your agency?
- What requirements must be addressed for your organization to contribute metrics data to enable performance measurement against peers?

# Benefits of CIS Membership



## **Benefits of Membership:** *CIS Benchmarks and Tools*

**CIS Members may use and distribute the Benchmarks and Audit Tools throughout their organizations.**

*In contrast, Non-CIS Members and their employees may use the CIS Benchmark and Tools ONLY on the host system onto which they are downloaded from the CIS public web site.*

**CIS Members receive two hours per month of free Benchmark/Audit Tool implementation support**

## Benefits of Membership: *Security Metrics Initiative*

CIS Members will be able to generate reports and graphs that compare their security outcomes with those of other organizations based on criteria such as conformity with standards, use of certain best practices, resource allocation, etc.



## Benefits of Membership: *Additional Benefits*

- **CIS Members Site** – *Unlimited number of Member employees have access to the CIS Members' website for:*
  - XML Benchmark versions;
  - CIS Configuration Assessment Tool (CIS-CAT); and
  - Participation on the Member discussion forums
  - Register at <http://members.cisecurity.org>
- **CIS Member Updates** - *Ad Hoc and Quarterly notification of new releases & updates to the Benchmarks and CIS-CAT*
- **CIS Member Trademark** - *Right to use the CIS Member Trademark*

[www.CISecurity.org](http://www.CISecurity.org)

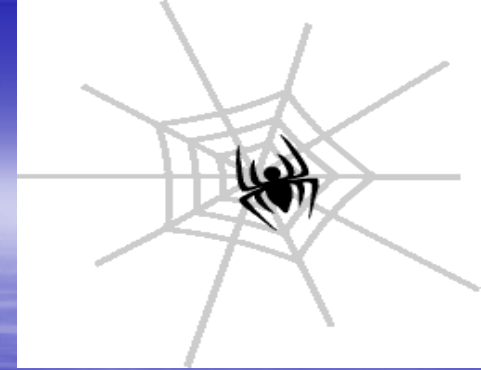


# **Playing Safely in the Cloud**

**Marie Greenberg**

**Marie Greenberg, CISSP, IAM, IEM  
Information Security Manager  
Virginia State Corporation Commission**

**“Come into my parlor.” said  
the spider to the fly.**



**Every day, government agencies are moving  
business practices from the physical realm into the  
cloud. Pay your taxes, renew your drivers license,  
incorporate your small business, order your birth  
certificate, look up a state employee...**

**As a public entity we have certain responsibilities  
to the citizens of Virginia. The public looks to us for  
guidance and assumes that the service we are  
providing is secure.**



# What can we do to make “Playing Safely in the Cloud” a reality for our Citizens?

**Assure the public that we have a secure site for them to conduct e-government business.**

**Require all users to register on our sites.**

**Verify the identity of users.**

# Bring awareness to the Citizens

## COV Citizen Awareness Banner

<http://www.vita.virginia.gov/security/default.aspx?id=5146>

The security of your personal information is important to us!

Diligent efforts are made to ensure the security of Commonwealth of Virginia systems. Before you use this Web site to conduct business with the Commonwealth, please ensure your personal computer is not infected with malicious code that collects your personal information. This code is referred to as a keylogger. The way to protect against this is to maintain current Anti-Virus and security patches.

For more information on protecting your personal information online, refer to the Citizens Guide to Online Protection.

# **Establish good Security Practices**

**Ensure secure payment services are in place.**

**Use a third party to evaluate the security of the web site.**

# **What can we do within our organizations to be more secure?**

**Identify the internet threats facing us.**

**Take ownership.**

**Promote a 'culture of security awareness'.**

**Create and maintain a security policy.**



**Take steps to protect our systems  
and data.**

**Keep software up-to-date.**

**Develop a disaster recovery plan.**

**Be proactive.**

# Playing Safely in the Cloud


Online Identity Management  
Web Application Security

**Steve Werby**  
Information Security Officer  
Virginia Commonwealth University

Anything you upload to  
a public website is not  
private – it's public.







## Sheryl

[facebook status not set]

**Networks:** Harvard, Facebook, Google


**Sex:** Female


**Interested In:** Not specified

**Relationship Status:**

**Birthday:**

**URL:** *not chosen yet!*

View Photos of Me 

Visit Facebook profile 

Profile Views: 00000002

**Find My Friends** ★

**Awards (0)** ★






Send Sheryl an Award

Poor Sheryl Sandb... has no Awards!

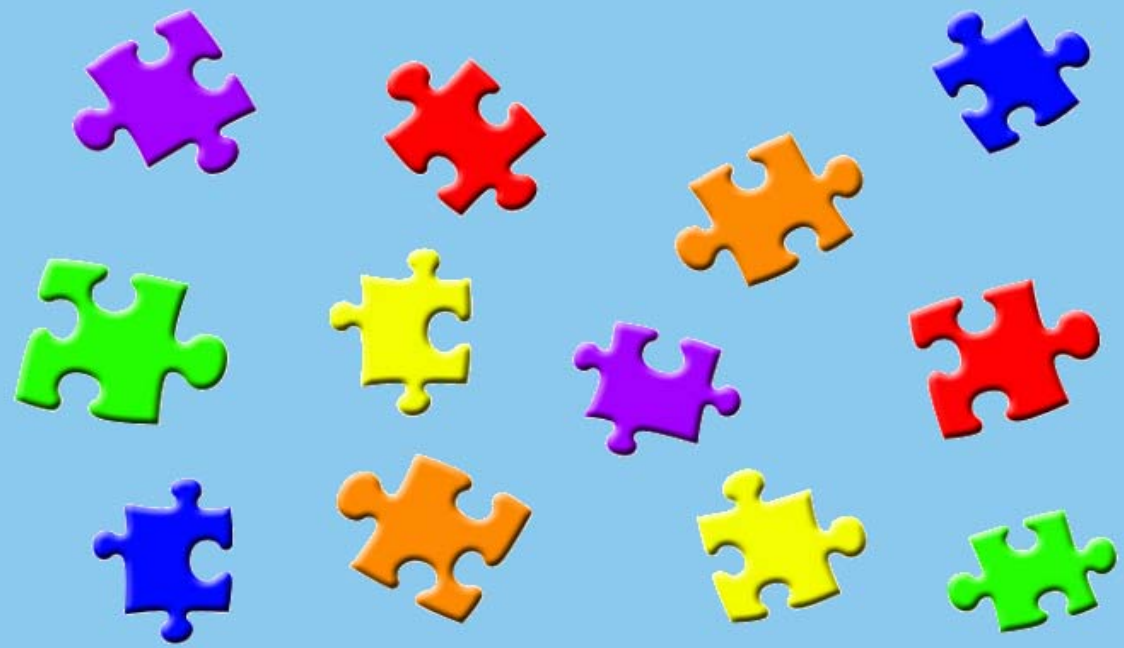
[Click here to give Sheryl Sandb...](#) an Award right

playing with my children  
things that  
interesting  
Crowd poetry  
Dixie Chicks  
A Wrinkle in Time  
Counting Crows  
politics  
Random  
Activities  
Movies  
Music

**Top Friends** ★





## Identity Theft



City / State  
**Email Address**  
Interests  
Activities  
Friends  
**Age**  
**Website**



First Name  
Last Name  
Friends  
Colleagues  
Interests  
Activities



First Name  
Last Name  
**Alias**  
Colleges  
Degrees  
Employers  
Job Titles  
**Email Address**  
Friends  
Colleagues



**Alias**  
City / State  
Friends  
Colleagues  
**Website**

## Social Engineering



**Email Address**



**Email Address**



**Alias**  
**Email Address**  
Interests

## Phishing

## Reconnaissance



First Name  
Last Name  
**Email Address**  
**Birthday**  
Street Address  
City / State  
Phone Number  
**Website**  
Marital Status  
Colleges  
Degrees  
Friends



First Name  
Last Name  
**Alias**  
**Age**  
City / State  
**Website**  
Marital Status  
Friends  
Interests  
Activities

friendfeed

maymz

Second | Brain™  
data 2



## Aggregate social network data

- Your personal lifestream
- Your connections' lifestreams

profilactic

socialthing!



Is the concept of privacy outdated?





1. Manage your identity

2. Make informed decisions

3. Voice your concerns

4. See #1

SaaS

Web 2.0

3G, 802.11n, mesh

Russian Business Network, Rock Phish

Cybercrime

IE, Firefox, Chrome, Safari, Opera

HIPAA, PCI, GLBA, FACTA, FERPA

Phishing, Smishing, Vishing

Blackberry, iPhone, Windows Mobile

AJAX

# Injection Flaws

Malicious File Execution

Failure to Restrict URL Access

Insecure Direct Object Reference

Cross Site Scripting (XSS)

Information Leakage / Improper Error Handling

Cross Site Request Forgery (CSRF)

Insecure Communications

Insecure Cryptographic Storage

Broken Authentication and Session Management



1. Know your web applications

2. Know your data

3. Secure **EVERYTHING**

4. Educate, educate, **EDUCATE**





*Virginia Information Technologies Agency*



# Commonwealth Security Information Resource Center

**Michael Watson**  
Security Incident Management Director

---





## What is a honeypot/honeynet?

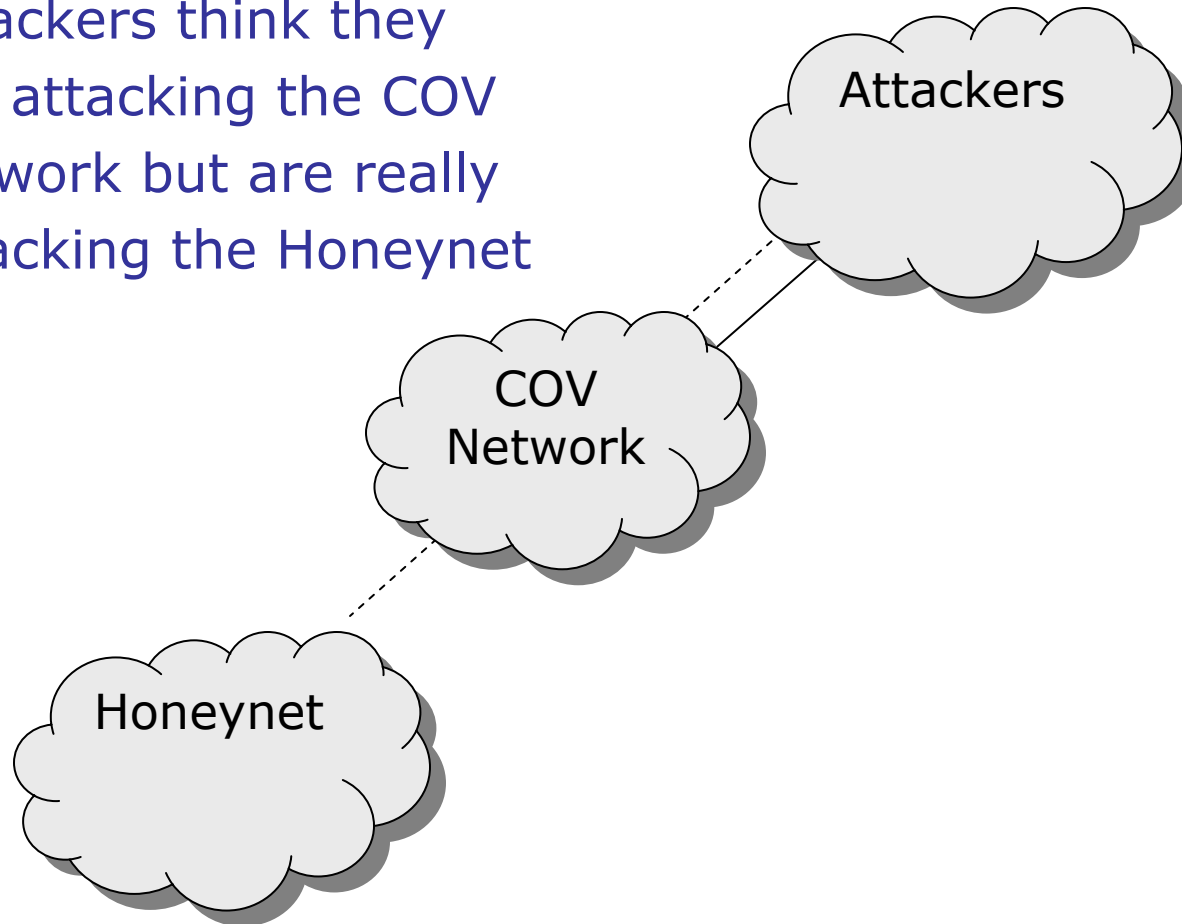
*A **honeypot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.*

*Typically a **honeynet** is used for monitoring larger and more diverse networks in which one honeypot is not sufficient.*

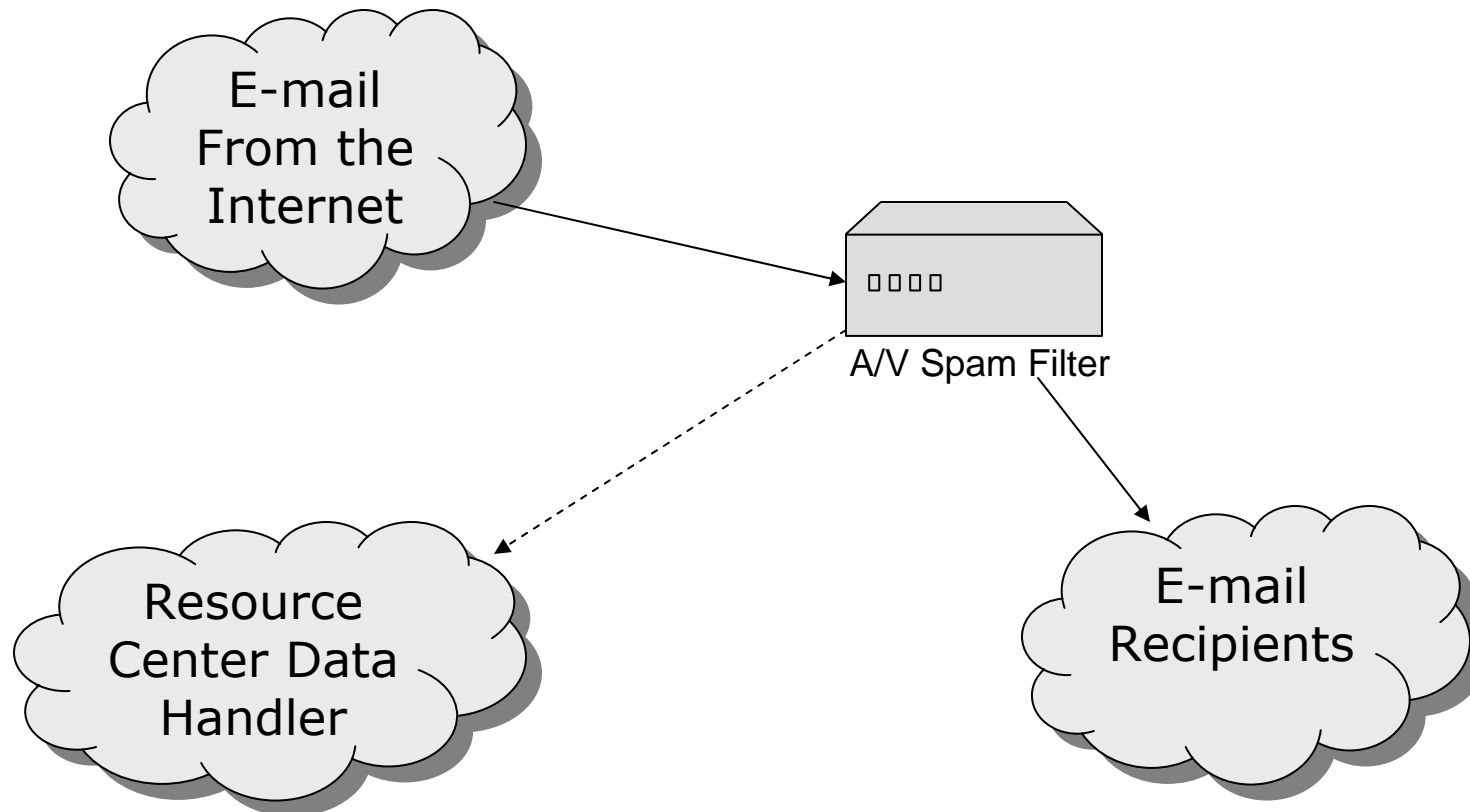
*-wikipedia.org*

# Honeynet Diagram

Attackers think they are attacking the COV network but are really attacking the Honeynet



# E-Mail Configuration







## Why run a honeypot?

- To better know your enemy
  - Who, where, what, how...
    - Targeted, Automated, Capture
- To better know your landscape
  - Network, OS, Applications
    - Vulnerabilities, Defenses
- Early warning & deterrence
  - Internal and external
    - Catch and capture malware.
- Research
  - Geopolitical, ISP, Prevalence
    - Worst offenders, rampant code

So it is said that if you know your enemies and know yourself, you will fight without danger in battles.

If you know only yourself, but not your opponent, you may win or you may lose.

If you know neither yourself nor your enemy, you will always endanger yourself.

- Sun Tzu



# What information can be captured?

- IP Addresses – Source and Destination
- Corporate owner of the IP (ISP/Net block)
- Geolocation – Country, City, Lat & Long
- Timestamps – When did this occur
  - How many times? Histogramming...
- Type of attack – Exploit/Vulnerability
- Malicious Code – Infected with...?
  - MD5/SHA-256 Hash



# Purpose of the Resource Center

- Two Main Goals
  - Create a place to provide security information that is relative to the Commonwealth
    - Includes security topics within the COV government
    - Addresses topics for those with interests in the security community
      - Citizens, businesses, other states, etc.
  - Create a source for providing threat data to third parties
    - Summary threat data for public viewing
    - Detailed threat data available for appropriate parties



## Hasn't this been done before?

- Scope is limited to a significant portion of Virginia government.
- The partnership between Virginia and Northrop Grumman allows comprehensive monitoring
  - Large attack surface area
  - Proper equipment and staffing for monitoring
  - Correlation from centralized log collection
- Analysis is specific to what attacks are directed at the Commonwealth





# Security Information

- Types of information posted
  - Security advisories
    - Advisories affecting the Commonwealth government computing environment
  - Phishing scams
    - Attempts to gather information from users that will be useful for malicious activity
  - Information security tips
    - How to integrate security into daily activity
  - News
    - The latest news about information security that would be useful to the government and its constituents
  - Threat data
    - Information showing statistics about the top attackers targeting the Commonwealth.



# Threat Data

- Threat Data
  - Malware collected by the honeynet
    - A copy of each piece of malware is kept for analysis
  - Attack data collected by the honeynet
    - The information about how the attack was performed is stored
  - Malicious mail data sent into the COV
    - When mail gateway security functions are triggered the malicious email is analyzed
  - Malware analysis information
    - When the malware was seen and how often it is used.
  - Visual representations of collected data
    - It helps show a global view of malicious activity



## Current Environment

- Consists of Honeynet
  - Listening on 1578 different addresses spanning 7 different networks
  - Collects malware
  - Collects attack information
- Central Spam/AV Mail Filter
  - A large portion of the agencies within the Commonwealth traverse this device
  - Collects data about each mail message
    - Virus type
    - Mail route
    - Destination of email



## Future Environment

- Honeynet
  - Expand listening addresses
  - Fingerprint the attack
  - Provide malware analysis and the impact on the Commonwealth environment
  - Additional visual representation of information
- Add Reporting Sources
  - Internet content filter data
  - IDS reporting information
  - Security incident data points
  - SQL injection data





# Current Information Security Climate

- Remediate the target
  - Antivirus scans
  - Anti-phishing protection
  - Spyware removal and detection
- Continued protection requires reliance on “doing the right thing”
  - Don’t click on the link
  - Don’t open the attachment
  - Don’t respond to anyone from Nigeria
  - Don’t trust anyone or anything
- Motivators
  - The bottom line
  - Personal agenda (i.e. hacktivism)



# The Information Security Climate Change

- Remediate the source
  - Identify participants
  - Understanding the attack types
  - Establish and counter motivators for the attacks
    - Consequences
    - Remove benefits
- Reduce the threats
  - Reduce reliance on users to behave properly
- Remove the motivators
  - Prevent desirable results



# Establishing an Attack Profile

- First step in remediating the source
- Determine an attacks source
  - Establish where the attacks originate from
- Understand the malware used
  - Look for similarities between malware or malware behavior
  - Link malware to a central point
  - Review how malware operates
- Establish patterns in attack vectors
- Know what effect it will have on the environment
- After establishing a profile it is easier to understand how to effectively stop the source



# Helpful Tools for Establishing a Profile

- Google
- Sandbox
  - An environment where it is possible to safely run programs. Often these programs are untested code, or untrusted programs from third-parties who may be malicious
  - Can be configured to watch a program execute
- Virustotal
  - Displays antivirus engines detecting the malware.
- Whois and Arin.net
  - Helps to tie the address back to a person or organization





## Who is Responsible?

organization: ORG-hA75-RIPE  
org-name: Technologii Maybutnego LLC, Hosting.UA  
address: Ukraine, Odessa, Gogolya 23

person: Top Management  
address: Technologii Maybutnego LLC  
46 Dalnickaya str  
65001 Odessa  
Ukraine  
phone: +38 048 7282111  
e-mail: info@hosting.ua

person: Andrey Slusar  
address: Ukraine Odessa Gogolya 23  
address: Tehnologii Budushego LLC  
phone: +38 048 7282111  
phone: +38 048 7281518  
e-mail: abs@hosting.ua



## Now What?

- What is the attacker getting from your system?
  - VICTIM
    - GET /x.exe Host: 83.68.71.69:2295
  - ATTACKER
    - GET /index.php?id=jcpsmiqnggelhh&scn=4&inf=0&ver=19&cnt=USA
    - Host: citi-bank.ru
- Local environment effect discovered
- Possibly involve law enforcement at this point.



# Putting the Data in Perspective

- Correlating the data
  - Relationships
    - Timelines
    - History/Trending
  - Patterns
    - Review attack profiles
      - Source addresses
      - Geographic location
  - Verification
    - Extremely difficult and often not possible
    - Often involves leaving the infrastructure in place
- Record everything
  - Data may be required by law enforcement



# Integrating Law Enforcement

- The second goal of resource center
  - Help law enforcement find an entry point
- Important in removing the source of the problem
- Plan for integration from the beginning
  - Determine the most useful data sets
- Example of results
  - Darkmarket.ws
  - TJX



# Questions?

Link to Commonwealth Security Information Resource Center:

[www.csirc.vita.virginia.gov](http://www.csirc.vita.virginia.gov)

Thank you!





*Virginia Information Technologies Agency*



# Cleaning Up SQL Injection

**Michael Watson**

Security Incident Management Director





# SQL Injection Overview

- Requirements
  - Web application that accepts input
  - Input used to create a SQL statement
  - Data input that isn't checked
- Results
  - Web page displaying unintended data
  - Unauthorized data in database
  - Potential database/system compromise



# Containing the Injection

- Site availability
  - Understand criticality
  - Reference risk management documents
    - Business Impact Analysis
- Understanding the risk
  - What data is in the database
  - What is the scope of access
  - Who is accessing the site



## Step 1: Contact COV Security

- Report the issue as a security incident
- We can help diagnose the issue
  - Help to define the scope
  - Help understand potential impacts
- Gather information
  - Allows us to associate data with any other incidents
  - Establish the attackers objective



## Step 2: Restrict Access

- Review site logs
  - Establish the injection points to determine the pages affected
    - COV log parsing
- Web site access
  - Restrict browsing to the site
    - Block at the network level – Firewall
    - Block at the web server level
- Database access
  - Restrict the database user
    - Prevent any data write operations
    - Remove any execute permissions





## Step 3: Clean up and Fix Injection Point

- Make sure the incident is contained and proper cleanup occurs
  - Review vulnerable web site for unchecked input
  - Review logs for any other suspicious activity
  - Remove malicious entries from the database
- Apply secure development practices
  - Check data for expected input
  - Make sure appropriate permissions are in place



## Step 4: Return to Normal Operations

- Put fixed code into production
- Continue to review logs
  - Look for abnormal activity
  - Review for abnormal database entries



## Step 5: Predict the Future

- Review other sites and check for similar issues
- Review the response process
  - Have a lessons learned with appropriate parties
- Update application/system criticality levels if appropriate
- Provide feedback
  - Let COV security know if we can be of any additional help



# Questions

Questions?



# ITP Security UPDATE & Questions

Bill Ross



***NORTHROP GRUMMAN***





*Virginia Information Technologies Agency*



# Coming Soon! New Guidelines

**Cathie Brown, CISM, CISSP**  
Deputy Chief Information Security Officer

---





## Policies, Standards & Guidelines... oh my

- There are 10 areas covered in the COV Information Security Policy and Standard and the Information Security Audit Standard.
- Our goal is to publish guidelines for each area to assist agencies with compliance efforts.

1. Risk Management	6. IT Security Audit
2. Data Protection	7. Personnel Security
3. Contingency Planning	8. Systems Security
4. Logical Access Control	<b>9. IT Facilities Security</b>
5. Threat Management	<b>10. IT Asset Management</b>



# IT Facilities Security Guideline

- Topics Covered
  - IT Facilities Security
    - Physical security controls must be in place to safeguard the facilities that house COV Information Technology (IT) equipment, systems, services, and personnel.
  - Roles and Responsibilities
    - The agency should document or have their service provider document the agency's IT facilities security components.



# IT Facilities Security Guideline

- Topics Covered – continued
  - IT Facilities Security Practices and Safeguards
    - Safeguarding IT Systems and Data
    - Safeguards to Protect Against Human, Natural, and Environmental Risks
    - Environmental Controls for IT Systems and Data
    - Physical Access Protection
    - Least Privilege Physical Access
    - IT System Monitoring and Auditing
    - IT System Physical Access Review
- **Appendices**
  - IT Facility Access Policy Example and Template
  - IT FACILITY SECURITY ASSESSMENT EXAMPLE and TEMPLATE



# IT Asset Management Guideline

- Topics Covered
  - IT Asset Management
    - IT Asset Control
    - IT Asset Removal Control
    - Control of Personal IT Assets
    - Data Removal from IT Assets
    - Inventory of Agency Hardware and Software Assets
  - Software License Management
    - Software License Management Practices
    - Use of Software
    - Software License Agreements
  - Configuration Management and Change Control
  - Appendices
    - Sample IT Asset Management Policy
    - Example and Template IT Asset Inventory





## Summary

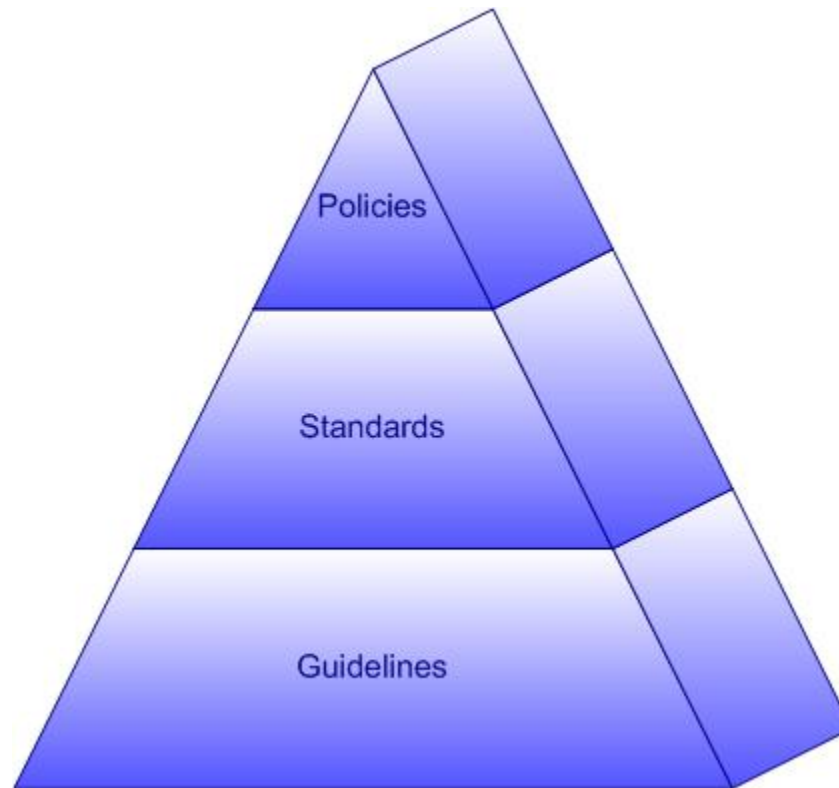
# Coming to ORCA Soon!

- IT Facilities Security Guideline
- IT Asset Management Guideline

<https://apps.vita.virginia.gov/publicORCA/default.asp>



# Questions and/or Comments?



**Thank you!**



*Virginia Information Technologies Agency*



# Commonwealth Security Annual Report

**Peggy Ward**

Chief Information Security and  
Internal Audit Officer

---





## § 2.2-2009

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

- C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.



## Explanation

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	1 of 1

### Agency

- Agency Abbreviation

### Security Audit Plan Rec'd

- Indicates whether agency has submitted a Security Audit Plan to Commonwealth Security and Risk Management for all systems classified as sensitive based on confidentiality, integrity, or availability.
- Options: Current = Received and up to date, No = Not Received, Outdated = Audit Plan was submitted but requires update, Extension Expired = An Exception was filed but has expired and Audit Plan has not been Received, Exception = A current exception is on file with Commonwealth Security and Risk Management.

### ISO Designated

- Indicates whether agency head has designated an Information Security Officer for the agency and provided the person's name, title and contact information to VITA no less than biennially.
- Options: YES/NO

### Attended IS Orientation (Extra Credit)

- Indicates the number of attendees that an agency has sent to attend Information Security Orientation.
- This data point is an "Extra Credit" data point where as it is not currently a requirement, but attendance is highly encouraged for ISO's and all interested parties.
- Options: 0 - ∞





## Explanation – Continued

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
XYZ	Current	YES	1	YES	1 of 1

### CAP's Rec'd

- Indicates whether the agency has submitted Corrective Action Plans (CAP's) for vulnerabilities identified in Security Audits.
- \*Note\* CAP's are to be submitted to Commonwealth Security and Risk Management one month after the completion of an audit and updates submitted quarterly for open vulnerabilities.
- Options: YES = Agency performed Security Audits and submitted CAP's, NO = Agency's Security Audit Plan indicates Security Audit was scheduled but has not submitted CAP, N/A = Not applicable, either Agency did not have Security Audits scheduled to date or Agency has not submitted a Security Audit Plan.

### CAP's Status

- Indicates the number of Corrective Action Plans submitted and the number of Security Audits scheduled based on the Security Audit Plan.
- Options: [Numbers of CAP's received] of [number of Security Audits scheduled] (example - 1 of 1, 0 of 1, 1 of 2, etc...), N/A = either Agency did not have Security Audits scheduled to date or Agency has not submitted a Security Audit Plan.



## Secretariat: Administration

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
HRC	NO	YES	0	N/A	N/A
DGS	Current	YES	0	NO	0 of 3
DHRM	Current	YES	0	N/A	N/A
DMBE	NO	YES	2	N/A	N/A
EDR	Current	YES	3	N/A	N/A
CB	Current	NO	1	NO	0 of 6
SBE	Current	NO	1	NO	0 of 2



## Secretariat: Agriculture & Forestry

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
DOF	Current	YES	1	N/A	N/A
VDACS	Current	YES	30	Yes	1 of 1



## Secretariat: Commerce & Trade

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
DBA	NO	YES	2	N/A	N/A
BOA	Current	YES	1	NO	0 of 3
DHCD	Current	YES	0	NO	0 of 3
DMME	Current	YES	1	YES	1 of 3
DOLI	NO	YES	3	N/A	N/A
DPOR	Current	YES	1	NO	0 of 5
TIC	NO	NO	0	N/A	N/A
VEC	Current	YES	2	NO	0 of 6
VEDP	NO	YES	0	N/A	N/A
VHDA	NO	NO	1	N/A	N/A
VNDIA	NO	NO	0	N/A	N/A
VRA	NO	NO	0	N/A	N/A
VRC	EXTENSION EXPIRED	YES	2	N/A	N/A



## Secretariat: Education (excluding Higher Ed)

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
DOE	Current	YES	1	NO	0 of 5
FCMV	NO	YES	0	N/A	N/A
GH	NO	YES	0	N/A	N/A
JYF	Current	YES	1	NO	0 of 3
LVA	Current	YES	1	N/A	N/A
SCHEV	EXTENSION EXPIRED	YES	0	N/A	N/A
SMV	NO	YES	0	N/A	N/A
VCA	NO	NO	0	N/A	N/A
VMFA	Current	YES	2	YES	2 of 2





## Secretariat: Education (Higher Ed only)

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
CNU	Current	YES	0	N/A	N/A
GMU	Current	YES	1	YES	6 of 22
JMU	Current	YES	0	YES	1 of 1
LU	Current	YES	1	YES	2 of 2
NSU	NO	YES	2	N/A	N/A
ODU	Current	YES	1	YES	4 of 4
RU	Current	YES	0	N/A	1 of 1
UMW	Current	YES	1	NO	0 of 1
VCCS	Current	YES	3	YES	1 of 2
VMI	Current	YES	0	NO	0 of 2
VSU	Current	YES	3	N/A	N/A



## Secretariat: Finance

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
DOA	NO	YES	4	N/A	N/A
DPB	Extension Expired	Yes	2	N/A	N/A
TAX	Current	YES	1	YES	11 of 16
TRS	Current	YES	2	NO	0 of 9



## Secretariat: Health & Human Resources

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
DHP	Current	YES	0	N/A	N/A
DMAS	Current	YES	6	YES	4 of 5
DMHMRSAS	Current	YES	13	N/A	N/A
DRS	Current	YES	0	NO	0 of 5
DSS	Current	YES	2	NO	0 of 18
TSF	NO	NO	0	N/A	N/A
VDA	Current	YES	1	N/A	N/A
VDH	Current	YES	3	YES	10 of 21



## Secretariat: Natural Resources

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
DCR	Current	YES	1	YES	1 of 2
DEQ	Current	YES	4	YES	1 of 1
DGIF	NO	YES	1	N/A	N/A
DHR	Current	YES	2	N/A	N/A
MRC	Current	YES	1	YES	4 of 4
VMNH	NO	YES	1	N/A	N/A



## Secretariat: Public Safety

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
ABC	Current	YES	1	YES	5 of 5
CASC	NO	NO	0	N/A	N/A
DCJS	Current	YES	2	NO	0 of 5
DFP	NO	YES	1	N/A	N/A
DFS	Current	YES	1	N/A	N/A
DJJ	Current	YES	3	NO	0 of 1
DMA	NO	NO	0	N/A	N/A
DOC	Current	YES	3	NO	0 of 6
DOCE	NO	YES	1	N/A	N/A
DVS	NO	YES	1	N/A	N/A
VDEM	NO	YES	1	N/A	N/A
VSP	Current	YES	3	N/A	N/A





## Secretariat: Technology

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
CIT	Current	YES	1	NO	0 of 1
VITA	Current	YES	35	YES	1 of 6



## Secretariat: Transportation

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
DMV	Current	YES	2	NO	0 of 8
DOAV	NO	YES	2	N/A	N/A
DRPT	Current	YES	1	N/A	N/A
MVDB	NO	YES	0	N/A	N/A
VDOT	Current	YES	5	YES	2 of 2



## Independent Branch Agencies

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
IDC	NO	YES	4	N/A	N/A
SLD	NO	YES	2	N/A	N/A
SCC	YES	YES	3	N/A	N/A
VCSP	YES	YES	3	N/A	N/A
VOPA	NO	YES	0	N/A	N/A
VRS	YES	YES	2	N/A	N/A
VWCC	Exception	YES	0	N/A	N/A



## Other

Agency	Security Audit Plan Rec'd	ISO Designated	Attended IS Orientation (Extra Credit)	CAP's Rec'd	CAP's Status
GOV	Exception	YES	2	N/A	N/A
OAG	NO	YES	1	N/A	N/A



# Questions?







*Virginia Information Technologies Agency*



# Upcoming Events

---





## UPCOMING EVENTS! 10/28

### CIO-CAO Meeting:

Formally known as AITR

**Tuesday, October 28th, 8:30 am**



# UPCOMING EVENTS! 10/29

## IS Orientation

**Wednesday, October 29th, 1:30 pm to 4:00 pm @ CESC**

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV IT Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

To register email [VITASecurityServices@vita.virginia.gov](mailto:VITASecurityServices@vita.virginia.gov)



## UPCOMING EVENTS! 11/17

### Commonwealth Information Security Council Meeting

**Monday, November 17<sup>th</sup>**, 12:00 - 2:00 p.m. @ CESC with Committee meetings from 2:00 – 3:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to [VITASecurityServices@vita.virginia.gov](mailto:VITASecurityServices@vita.virginia.gov) (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at:  
<http://www.vita.virginia.gov/security/default.aspx?id=5128>



# UPCOMING EVENTS! 11/19

## NEXT ISOAG MEETING!

**November 19th, 1:00 – 4:00 pm @ CESC**

## DRAFT AGENDA

**Information Security Issues – Ken Blotteaux (NCFTA) & Donna Gregory (IC3)**

**Electronic Content Management – Herb Ward, DEQ**

**ARMICS – Joe Kapelewski (DOA)**

**Security Incident Reporting – Michael Watson & Don Kendrick, VITA**





*Virginia Information Technologies Agency*



**Any Other Business ??????**

---



# ADJOURN

## THANK YOU FOR ATTENDING!!

